UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/784,897	02/24/2004	Ronald Anton De Jongh	18949.002	1012

27890 7590 10/05/2007

STEPTOE & JOHNSON LLP
1330 CONNECTICUT AVENUE, N.W.
WASHINGTON, DC 20036

EXAMINER	
HOLLOWAY III, EDWIN C	
ART UNIT	PAPER NUMBER
2612	
MAIL DATE	DELIVERY MODE
10/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/784,897	DE JONGH, RONALD ANTON	
	Examiner	Art Unit	
	Edwin C. Holloway, III	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,12,14-19,21-26 and 28-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8, 12, 14-19, 21-26, 28-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892) ✓

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

EXAMINER'S RESPONSE

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6-5-07 and supplemental filed 7-23-07 have been entered. Claims 1-8, 12, 14-19, 21-26, 28-33 are pending. The examiner has considered the presentation of claims in view of the disclosure and the present state of the prior art. And it is the examiner's position that the claims are unpatentable for the reasons set forth in this Office action:

Drawings

2. The drawings are objected to because page 11 line 17 of the spec discloses that the screens do not have repeating characters, such as "no two number 3's," but fig. 3 shows two number 3's and the 2nd, 4th and 5th screen in fig. 6(a) have two number 5's.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application.

Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-8, 12, 14-19, 21-26, 28-33 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant has not identified support for the amended and new claims in the specification as originally filed, nor has applicant stated that no new matter has been added by the amendment. Support is lacking for at least "such that each variable is associated with a key different from the previous attempt" added to independent claims 1, 12, 21, 22, 23 and 24. Further, "wherein each individual key, which is associated to the combination of variables, is generated by a predetermined sequence, the predetermined sequence optionally changing after a predetermined period of time or a predetermined number of access attempts" in new claim 32 lacks support. Applicant should specifically point out support in the original disclosure for the new or amended claims. See MPEP 714.02 and 2163.06. The statement that support "can be found throughout the specification" is not sufficient because each variable associated with a different key

is contradicted by figs 1-2 showing number 9 assigned to the same key, fig. 3-4 showing at least number 6 assigned to the same key and fig. 6(a) showing at least number 0 assigned to the same key for different screens. Although page 12 line 13 of the spec includes "the combination of numbers is different," this does not support "each variable" associated with a different key as claimed.

Claim Rejections - 35 USC § 102 & 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1-8, 12, 14-19, 22-24, and 28-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maddalozzo, Jr. et al. (US 6,434,702) in view of Morgan et al. (US 5,274,370).

Referring to claims 1, 12, and 22-24, Maddalozzo teaches a method that provides security for a system using a virtual keypad (see Abstract). As called for in claims 1 and 22, Maddalozzo's method comprises (a) displaying a virtual keypad, which has a predetermined number (i.e., plurality, as called for in claim 22) of keys that enable a user to enter a password (i.e., secure access code), on a touchscreen surface (i.e., a graphical user interface, as called for in claim 22) (see Fig. 1, keypads 101-103; Fig. 2, keypads 102-103; Col. 2, lines 66-

67; Col. 3, lines 1-34 and 66-67; and Col. 4, lines 1-4), as called for in claims 1 and 22; (b) associating one character (i.e., variable) with each individual key, wherein the characters are shuffled (i.e., one or more variables change) after each utilization or at different intervals (see Col. 3, lines 13-34 and 45-59; Col. 4, lines 49-67; and Col. 5, lines 23-27), as called for in claims 1 and 22; (c) associating different characters with different keys after each attempt to input a password (i.e., associating different variables with different key for different attempts to input the secure access code) (see Fig. 3, steps 308-309; Col. 3, lines 13-34 and 45-59; Col. 4, lines 49-67; and Col. 5, lines 23-27), as called for in claim 1; (d) a user selecting each key that corresponds to the character of the password (see Fig. 3, steps 301-306; Col. 3, lines 13-34; Col. 4, lines 14-49; and Col. 5, lines 4-22), as called for in claims 1 and 22; (e) comparing the characters associated with each selected key to the characters of the password with a code stored in a security code check mechanism's database (see Fig. 3, steps 305 and 306; Col. 4, lines 32-48; and Col. 5, lines 18-23), as called for in claim 1; and (f) allowing the user to access electronic services provided by the automatic teller machine (ATM) associated with the keypad if the characters associated with the keys, as sequentially selected by

the user, match the stored code (see Fig. 3, step 307; Col. 1, lines 27-31; Col. 3, lines 13-15; Col. 4, lines 48- and 49; and Col. 5, lines 22-23), as called for in claim 1. Regarding claim 12, as shown in Figs. 1 and 2, Maddalozzo's virtual keypad comprises (a) a static framework of virtual keys (i.e., a predetermined number of virtual keys) (see Figs. 1 and 2; Col. 3, lines 66-67; and Col. 4, lines 1-4); and (b) a predetermined character associated with each virtual key, wherein a user selects a virtual key based on whether the character associated with the virtual key matches the corresponding character in the user's password (i.e., access code) (see Fig. 3, steps 308 and 309; Col. 4, lines 32-63; and Col. 5, lines 23-27). Though the characters are assigned randomly after each access, the assignment of a character to a virtual key is understood to be predetermined since the reshuffled characters are translated into a physical location, and a keypad code mechanism saves the new character configuration, which is then used during a new access attempt (see Col. 4, lines 31-56 and Col. 5, lines 23-27). Regarding claim 23, Maddalozzo teaches an ATM terminal (i.e., a secure access terminal) comprising (a) a touchscreen (i.e., graphical interface) that allows a user to access secured electronic information (see Col. 2, lines 66-67; Col. 3, lines 1 and 13-15; Col. 4, lines 44-49; and Col. 5, lines 18-23); and

(b) a plurality of virtual keys displayed on the touchscreen, each virtual key associated with one character (i.e., variable), wherein different characters are associated with different keys after each attempt to input a password (see Figs. 1 and 2, virtual keypads 101, 102, and 103; Fig. 3, steps 308-309; Col. 3, lines 13-34, 45-59, and 66-67; Col. 4, lines 1-4 and 49-67; and Col. 5, lines 23-27). As called for in claims 22 and 23, Maddalozzo teaches creating a new look-up table that maps randomly arranged characters with their physical location at step 308 in Fig. 3 after each time the ATM has been accessed (see Col. 4, lines 35-48 and Col. 5, lines 4-11 and 23-27). Though Maddalozzo fails to disclose selecting the characters (i.e., assigning a set of variables to the plurality of virtual keys, as called for in claim 23) from a predetermined set listed in a table containing all possible combinations of variables and virtual keys (as called for in claim 22) without any repetition of variables (as called for in claim 23), the Examiner takes Official Notice that the use of look-up tables is well known. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Maddalozzo's method and ATM such that the characters are selected from a predetermined set of combinations listed in a table containing all possible combinations of characters and

virtual keys without any repetition of the characters because a look-up table containing all possible combinations of characters and virtual keys eliminates the need to create a new look-up table that maps randomly arranged characters with their physical location after each time the ATM has been accessed, thereby making the system more efficient. Regarding claim 24, Maddalozzo's method lacks the step of inserting a bank issued card into an ATM terminal to execute banking transactions. Maddalozzo's method, however, does include the step of a user entering his or her PIN into an ATM terminal (see Col. 1, lines 27-31 and Col. 3, lines 13-34), which occurs after a user inserts his or her ATM card into the ATM terminal; thus, Maddalozzo's method does include (a) a user inserting a bank issued card into an ATM terminal. Maddalozzo's method further includes (b) creating a virtual keyboard by assigning a character to each virtual key, wherein different characters are associated with different keys after each attempt to input a password (i.e., a predetermined number of access attempts) (see Figs. 1 and 2, virtual keypads 101, 102, and 103; Fig. 3, steps 308-309; Col. 3, lines 13-34, 45-59, and 66-67; Col. 4, lines 1-4 and 49-67; and Col. 5, lines 23-27); (c) displaying the virtual keypad (see Fig. 3, step 309; and Col. 5, lines 23-27); and (d) requesting the access code be entered into the virtual

keypad since Maddalozzo teaches a user knowing when to enter his or her password (see Col. 3, lines 19-22; Col. 4, lines 13-16, 32-34, and 53-59; and Col. 5, lines 4-23).

Maddalozzo, however, fails to teach the following: (1) associating at least two variables with each individual key (as called for in claims 1, 12, and 22-24); and (2) associating different combinations of variables, each being different (i.e., not repetition), with different keys after each attempt to input a password (as called for in claims 1, 12, and 22-24).

In an analogous art, Morgan's method comprises (a) providing five keys 68, 70, 72, and 74 (i.e., a predetermined number of keys) used to input an access code (see Fig. 9 and Col. 8, lines 17-30); (b) associating two variables with each key (see Col. 8, lines 17-30 and 53-59); (c) random assignment (or at lest full well scrambled assignment) of digits 0 through 9 to the display, or alternatively the digits 0 through 4 to the left displays 80, 82, 84, 86, and 88 and randomly assigning digits 5-9 to the right displays 90, 92, 94, 96, and 98 (i.e., associating different combination of variables with different keys) (see Col. 8, lines 53-59); (d) selecting, by a user, each key 68, 70, 72, or 74 that corresponds to one of the variables of the access code (see Col. 5, lines 46-48 and 57-60); (e) comparing the values associated with each selected key and with

a code stored in a database (see Col. 5, lines 57-60); and (f) allowing the user access if the values associated with the selected keys, as sequentially selected by the user, match the stored code (see Col. 5, lines 57-60). Because Morgan teaches associating different variables with different keys after the system is turned on and for each new key entry of a full code (see Col. 4, lines 56-67 and Col. 5, lines 1-20), it is understood that digits 0 through 4 are randomly assigned to the left displays 80, 82, 84, 86, and 88 and digits 5-9 are randomly assigned to the right displays 90, 92, 94, 96, and 98 after each entry of a full code. In addition, each combination assigned to each key represents a different value (i.e., lacks repetition) since digits 0 through 4 are randomly assigned to the left displays 80, 82, 84, 86, and 88 and digits 5-9 are randomly assigned to the right displays 90, 92, 94, 96, and 98.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Maddalozzo's method, virtual keypad, and ATM as taught by Morgan because a virtual keypad having five keys and two characters assigned to each key provides high security by making it more difficult for an unauthorized person to observe and determine an authorized user's password (see Maddalozzo, Col. 1, lines 49-54; and Morgan, Col. 8, lines 49-66).

Regarding the amendment of the independent claims 1, 12, 22, 23 and 24 to add "such that each variable is associated with a key different from the previous attempt," this limitation would have been obvious in view of the "scrambled" assignment in col. 8 lines 53-59 of Morgan and the repositioning or "reshuffle" in col. 3 of Maddalozzo that one of ordinary skill in the would recognize as assigning each variable to a different key to scatter the keypad so that people spying on the user will not learn the password/code. Further, associating different combination of variables/characters with different key would have been obvious in view of the shuffle or scramble of Maddalozzo and Morgan "without using duplicate numbers" in col. 5 lines 1-20 of Morgan. Further, Morgan discloses the digits on the left and right may be similarly ordered such that 0 and 5, 1 and 6, etc. are always associated (paired) to aid operation (col. 8 lines 39-44), but if there is a chance of someone other than the user seeing one side but not the other side of the keyboard, then the fixed left to right display association (pairing) should not be used. Therefore, Morgan teaches associating different combinations of variables with different keys for different attempts to input the secure access code such that each variable is associated with a key different from the previous attempt. Note that applicant's fig. 6(a) appears to

show varying the digits on only one side of the keyboard that would have been obvious in view of Morgan disclosing ~~only~~ instance when an observer sees only one side of the display so that, obviously, only one side need be varied.

Regarding claim 2, Maddalozzo and Morgan teach that alphanumeric characters are assigned to each key (see Maddalozzo, Col. 3, lines 15-17; and Morgan, Col. 9, lines 11-17).

Regarding claims 3, 14, and 28, Maddalozzo and Morgan teach that numbers are assigned to each key (see Maddalozzo, Col. 4, lines 3-6; and Morgan, Col. 8, lines 27-30 and 53-59).

Regarding claims 4, 15, and 29, Maddalozzo and Morgan teach that letters are assigned to each key (see Maddalozzo, Col. 3, lines 15-17; and Morgan, Col. 9, lines 11-17).

Regarding claims 5, 16, and 30, Maddalozzo and Morgan teach that a combination of letters and/or numbers is assigned to each key (see Morgan, Col. 9, lines 11-17).

Regarding claims 6, 17, and 31, Maddalozzo and Morgan teach that symbols are assigned to each key (see Maddalozzo, Col. 3, lines 15-17; and Morgan, Col. 9, lines 11-17).

Regarding claims 7 and 18, Maddalozzo, as modified by Morgan, teaches creating a new table of combinations and then displaying the new keypad after each access attempt or after

every three access attempts (i.e., the predetermined number of access attempts) (see Maddalozzo, Col. 3, lines 45-47; Col. 4, lines 31-56; and Col. 5, lines 23-25). Though the characters are assigned randomly after each access, the assignment of the characters to a virtual key is understood to be predetermined since the reshuffled characters are translated into a physical location, and a keypad code mechanism saves the new character configuration, which is then displayed used during a new access attempt (see Maddalozzo, Col. 4, lines 31-56 and Col. 5, lines 23-27). Further, Maddalozzo includes a "predefined patter" or "pseudo-random" sequence in col. 3 lines 45-50 that is predetermined (known) pattern. In other words, Maddalozzo and Morgan's combination of characters is generated by a sequence that is predetermined prior to the combination of characters being displayed and that changes after a predetermined number of access attempts.

Regarding claims 8 and 19, as explained in the previous rejection of claim 7, Maddalozzo and Morgan's combination of characters is selected and then associated with the keys in accordance with a predetermined sequence of a combination of characters. Per Maddalozzo and Morgan, one combination of characters is displayed for each user (see Maddalozzo, Col. 4,

lines 31-67 and Col. 5, lines 23-27; and Morgan, Col. 8, lines 53-59).

Claim 32 would have been obvious for the same reasons applied above to claim 7 and because the display of Maddalozzo and Morgan are associated with individual keys.

Claim 33 would have been obvious for the same reasons applied above to claim 8 and because the display of Maddalozzo and Morgan are associated with individual keys.

7. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jalili (US 6,209,104) in view of Morgan et al. (US 5,274,370).

Referring to claim 21, Jalili teaches a display device 104 displaying display image 250 (see Figs. 4 and 5) comprising a group of icons i0-in 230 (see Col. 6, lines 32-37). The group of icons i0-in 230 forms a virtual keypad when display device 104 is a touchscreen device (see Col. 7, lines 21-24). Jalili's virtual keypad comprises (a) icons i0-in 230 functioning as virtual keys for a user to enter a password and being displayed via display device 104 (i.e., a graphical interface) in different arrangements and positions for each attempt at inputting information (see Col. 7, lines 7-14 and 21-24; and Col. 8, lines 22-32 and 46-49); and (b) a plurality of characters, each character associated with each icon i0-in 230

(see Col. 6, lines 41-47; Col. 7, lines 21-24; and Col. 8, lines 21-32). Because Jalili teaches that server subsystem 200 generates a series of icons i0-in 230 that include at least a user's password or personal identification number (PIN), wherein the icons' locations and features (i.e., character assignment) are (1) generated pseudo-randomly or according to a set scheme or (2) obtained from a filed, look-up table, database, etc. when a user identifies himself or herself (see Col. 8, lines 21-32), it is understood that different characters are associated with different icons after each access attempt. Jalili, however, is silent on associating at least two characters with each icon, wherein different character combinations are associated with each icon after each user's input attempt and each character in each combination represents a different value.

In an analogous art, as explained in the previous rejection of claims 1, 12, and 22-24, Morgan's keypad comprises (a) five keys 68, 70, 72, and 74 (i.e., a plurality of keys) used to input an access code, each key associated with two characters (see Fig. 9 and Col. 8, lines 17-30 and 53-59); and (b) a plurality of combinations associated with each key, wherein the combinations are determined random assignment (or at lest full well scrambled assignment) of digits 0 through 9 to the display, or alternatively by randomly assigning digits 0 through 4 to the

left displays 80, 82, 84, 86, and 88 and randomly assigning digits 5-9 to the right displays 90, 92, 94, 96, and 98 (i.e., associating different combination of variables with different keys) (see Col. 8, lines 53-59). Because Morgan teaches associating different variables with different keys after the system is turned on and for each new key entry of a full code (see Col. 4, lines 56-67 and Col. 5, lines 1-20), it is understood that digits 0 through 4 are randomly assigned to the left displays 80, 82, 84, 86, and 88 and digits 5-9 are randomly assigned to the right displays 90, 92, 94, 96, and 98 after each entry of a full code.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Jalili's virtual keypad as taught by Morgan because a virtual keypad having two characters assigned to each key provides high security by making it more difficult for an unauthorized person to observe and determine an authorized user's password (see Jalili, Col. 3, lines 61-67 and Col. 4, lines 1-5; and Morgan, Col. 8, lines 49-66).

Regarding the amendment of the independent claim 21 to add "such that each variable is associated with a key different from the previous attempt," this limitation would have been obvious in view of the "scrambled" assignment in col. 8 lines 53-59 of

Morgan and the repositioning or pseudo-random location/pattern in col. 8 lines 27-32 of Jalili that one of ordinary skill in the would recognize as assigning each variable to a different key to scatter the keypad so that people spying on the user will not learn the password/code. Further, associating different combination of variables/characters with different key would have been obvious in view of the different locations and features in col. 8 lines 27-32 Jalili and/or scramble "without using duplicate numbers" in col. 5 lines 1-20 of Morgan. It is also noted that in addition to the different random pattern of Jalili, different background and different icon shapes are provided in col. 9 lines 1-5, wherein the background and shapes are variables that at least suggest each variable associated with a key different from a previous attempt. Further, Morgan discloses the digits on the left and right may be similarly ordered such that 0 and 5, 1 and 6, etc. are always associated (paired) to aid operation (col. 8 lines 39-44), but if there is a chance of someone other than the user seeing one side but not the other side of the keyboard, then the fixed left to right display association (pairing) should not be used. Therefore, Morgan teaches associating different combinations of variables with different keys for different attempts to input the secure access code such that each variable is associated with a key

different from the previous attempt. Note that applicant's fig. 6(a) appears to show varying the digits on only one side of the keyboard that would have been obvious in view of Morgan disclosing ~~only~~ instance when an observer sees only one side of the display so that, obviously, only one side need be varied.

8. Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maddalozzo, Jr. et al. (US 6,434,702) in view of Morgan et al. (US 5,274,370) as applied to claim 24 above, and further in view of Chasko et al. (US 6,715,078).

Regarding claims 25 and 26, Maddalozzo, as modified by Morgan, teaches creating a new look-up table that maps randomly arranged characters with their physical location at step 308 in Fig. 3 after each time the ATM has been accessed (see Maddalozzo, Col. 4, lines 35-48 and Col. 5, lines 4-11 and 23-27). Though Maddalozzo and Morgan fail to disclose selecting the characters from a predetermined set listed in a table containing all possible combinations of variables and virtual keys without any repetition of variables (as called for in claim 25), the Examiner takes Official Notice that the use of look-up tables is well known. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Maddalozzo and Morgan's method such that the

characters are selected from a predetermined set of combinations listed in a table containing all possible combinations of characters and virtual keys without any repetition of the characters because a look-up table containing all possible combinations of characters and virtual keys eliminates the need to create a new look-up table that maps randomly arranged characters with their physical location after each time the ATM has been accessed, thereby making the system more efficient. Regarding claim 26, Maddalozzo and Morgan's method comprises (a) inputting a password (i.e., a personal access code) (see Maddalozzo, Col. 3, lines 19-22; Col. 4, lines 14-21 and 44-49; and Col. 5, lines 4-23); (b) verifying the password (see Maddalozzo, Fig. 3, step 306; Col. 4, lines 44-49; and Col. 5, lines 11-23); and (c) allowing a user to access various banking transactions (see Maddalozzo, Fig. 3, step 307; Col. 4, lines 48-49; and Col. 5, lines 11-23). Maddalozzo and Morgan fail to expressly teach (1) transmitting card information to a server (as called for in claim 25); (2) verifying the authenticity of the bank-issued card (as called for in claim 25); and (3) encrypting data representing the password and transmitting the data to a server (as called for in claim 26).

In an analogous art, Chasko's method comprises the steps of (a) inserting a bank-issued card into CTT 10's card clot 110 to

execute a transaction (see Col. 1, lines 21-26 and 40-55; Col. 3, lines 2-5; Col. 4, lines 4-6; and Col. 5, lines 27-35); and (b) displaying PIN entry area 102 to a user (see Col. 2, lines 48-62). Because Chasko teaches that CTT 10's microprocessor 130 processes a user's PIN and controls the content of the information displayed on flat panel touch screen 101 by using a standard ATM operating system and application program (see Col. 1, lines 21-26 and 40-55; and Col. 5, lines 27-35), it is understood that a user enters his/her PIN upon seeing a PIN request displayed on flat panel touch screen 101. As shown in Fig. 1A, PIN entry area 102 includes a predetermined number of icons, each icon having at least one variable associated therewith. Though Chasko fails to expressly teach associating at least two variables with each icon (as called for in claims 24 and 27), wherein the at least two variables are alphanumeric characters (as called for in claim 30), Chasko clearly shows associating as many as four variables (e.g., "7, P, Q, R, S") with one icon. In addition, Chasko teaches that PIN entry area 102's layout is predetermined during the programming design of the screen layout (see Col. 5, lines 3-9). Regarding claim 25, Chasko's method includes the step of (a) determining which PIN entry area 102 to display to the user, wherein PIN entry area 102 is determined during the programming design of the screen

layout (see Col. 5, lines 3-13). Chasko teaches that CTT 10's microprocessor 130 uses a standard ATM operating system and application program, wherein the ATM operating system and application program allow a user access to electronic services (such as cash withdrawals, funds transfer, and deposits) only if the user's PIN is valid to prevent unauthorized transactions; thus the authenticity of the card is verified prior to account access. Though Chasko's method does include the step of a user inserting a card into card clot 110 (see Col. 3, lines 2-4 and Col. 4, lines 4-6), Chasko omits expressly teaching the steps of transmitting the card information to a server. Since the applicant does not traverse the examiner's assertion of official notice that transmitting card information from an ATM to a server is well known, the well known in the art statement is taken to be admitted prior art. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chasko's method such that the ATM transmits a user's card information to a server because such step eliminates each ATM having to store and maintain a large database of customer accounts and provides a bank with centralized control of the system and database. Regarding claim 26, Chasko's method, as shown in Fig. 3, further comprises (a) a user entering a PIN at steps 302, 304, 308, 310, 314, and 318

(see Col. 6, lines 7-35); and (b) cryptographic smart card 114 encrypting the PIN at step 320 (see Col. 6, lines 35-42). Although Chasko omits expressly teaching that the user has access to a plurality of electronic services upon successful verification of the PIN, Chasko discloses that CTT 10 is used with ATMs and that CTT 10's microprocessor 130 processes a user's PIN and controls the content of the information displayed on flat panel touch screen 101 by using a standard ATM operating system and application program (see Col. 1, lines 21-26 and 40-55; and Col. 5, lines 27-35). Standard ATM operating systems and application programs allow a user access to electronic services (such as cash withdrawals, funds transfer, and deposits) only if the user's PIN is valid to prevent unauthorized transactions.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method of Maddalozzo and Morgan as taught by Chasko because a method comprising (1) transmitting card information to a server (as called for in claim 25); (2) verifying the authenticity of the bank-issued card (as called for in claim 25); and (3) encrypting data representing the password and transmitting the data to a server (as called for in claim 26) offers several advantages: (1) an ATM terminal that transmits a

user's card information to a server eliminates each ATM terminal having to store and maintain a large database of customer accounts and enables a bank to centrally control a plurality of ATM terminals; (2) security at an ATM terminal is further enhanced by requiring a user to provide a valid bank-issued card in addition to a password prior to accessing various banking transactions; and (3) the encryption of card information prior to transmission to the server makes it difficult for an unauthorized person to obtain an authorized user's password, thereby improving security of the ATM system.

Response to Arguments

9. Applicant's arguments filed 7-23-07 have been fully considered but they are not persuasive.

The argument that Maddalozzo has only one character associated with each key is not persuasive because Maddalozzo was not applied for this limitation. The rejection was based on a combination with Morgan to disclose two character assigned to an individual key. The argument that Maddalozzo lacks each variable associated with a respective key as well as each individual key are different form a previous attempt is not persuasive because Maddalozzo does disclose reshuffling the key assignments. The argument that Maddalozzo lacks each variable associated with a key different from a previous attempt is not

persuasive because Maddalozzo does disclose reshuffling the key assignments.

The argument that Morgan lacks each variable associated with a respective key as well as each individual key are different form a previous attempt is not persuasive because Morgan does disclose scrambling key assignments similar to the reshuffling of Morgan. The argument that Morgan lacks each variable associated with a key different from a previous attempt is not persuasive because Morgan does disclose scrambling the key assignments similar to the reshuffling of Maddalozzo. Further, Morgan discloses the digits on the left and right may be similarly ordered such that 0 and 5, 1 and 6, etc. are always associated (paired) to aid operation (col. 8 lines 39-44), but if there is a chance of someone other than the user seeing one side but not the other side of the keyboard, then the fixed left to right display association (pairing) should not be used. Therefore, Morgan teaches associating different combinations of variables with different keys for different attempts to input the secure access code such that each variable is associated with a key different from the previous attempt. Note that applicant's fig. 6(a) appears to show varying the digits on only one side of the keyboard that would have been obvious in view of Morgan disclosing ~~only~~ instance when an observer sees only one

side of the display so that, obviously, only one side need be varied.

The argument that Jalili, alone or combined with Morgan, lacks each variable associated with a key different from a previous attempt is not persuasive because this limitation would have been obvious in view of the "scrambled" assignment in col. 8 lines 53-59 of Morgan and the repositioning or pseudo-random location/pattern in col. 8 lines 27-32 of Jalili that one of ordinary skill in the would recognize as assigning each variable to a different key to scatter the keypad so that people spying on the user will not learn the password/code. Further, associating different combination of variables/characters with different key would have been obvious in view of the different locations and features in col. 8 lines 27-32 Jalili and/or scramble "without using duplicate numbers" in col. 5 lines 1-20 of Morgan. It is also noted that in addition to the different random pattern of Jalili, different background and different icon shapes are provided in col. 9 lines 1-5, wherein the background and shapes are variables that at least suggest each variable associated with a key different from a previous attempt. Further, Morgan discloses the digits on the left and right may be similarly ordered such that 0 and 5, 1 and 6, etc. are always associated (paired) to aid operation (col. 8 lines

39-44), but if there is a chance of someone other than the user seeing one side but not the other side of the keyboard, then the fixed left to right display association (pairing) should not be used. Therefore, Morgan teaches associating different combinations of variables with different keys for different attempts to input the secure access code such that each variable is associated with a key different from the previous attempt. Note that applicant's fig. 6(a) appears to show varying the digits on only one side of the keyboard that would have been obvious in view of Morgan disclosing ~~only~~ instance when an observer sees only one side of the display so that, obviously, only one side need be varied.

The argument that Chasko lacks each variable associated with a key different from a previous attempt is not persuasive for the reasons stated above.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Rehm (US 4502048) and Cairns (US 4962530) disclose security keyboards with randomly scrambled keys.

CONTACT INFORMATION

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edwin C. Holloway, III whose telephone number is (571) 272-3058. The

examiner can normally be reached on M-F from 9:00 to 5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian Zimmerman, can be reached on (571) 272-3059.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

EH
9/29/07
(571) 272-3058

EDWIN C. HOLLOWAY, III
PRIMARY EXAMINER
ART UNIT 2612